UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/725,821	11/29/2000	James D. Dworkin	SC11015ZC	4735

23125 7590 01/14/2005

FREESCALE SEMICONDUCTOR, INC.
LAW DEPARTMENT
7700 WEST PARMER LANE MD:TX32/PL02
AUSTIN, TX 78729

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 01/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/725,821	DWORKIN ET AL.	
	Examiner	Art Unit	
	Matthew T Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☒ Claim(s) *1-7* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on September 21, 2004.

DETAILED ACTION

1. Claims 1-18 have been examined.

Title

2. The title of the invention is acceptable

Priority

3. No foreign priority has been claimed in this application.

4. The effective filing date of the subject matter defined in the pending claims of this application is 11/29/2000.

Drawings

5. The drawings submitted on 11/29/2000 are acceptable for examination proceedings.

Claim Objections

6. Claims 1-7 are objected to because of the following informalities: Line 8 of Claim 1 recites "and and". Appropriate correction is required.

Claims 2-7 are objected to by virtue of their dependency to claim 1.

Appropriate correction is required.

Claim Rejections – 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> *The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.*

8. Claims 9-13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

9. Claims 9 and 13 recite the limitation "the summing circuit". There is insufficient antecedent basis for this limitation in the claim.

10. Claim 10 recites the limitation "the adder". The ordinary person skilled in the art would be unable to determine which adder claim 10 is meant to be referring to in line 5. This is due to the recitation of "an adder" in both claims 8 and 10. Therefore, claim 10 is rejected for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

11. Claims 11-12 are rejected by virtue of their dependency to claims 9 and 10.

Claim Rejections – 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

13. Claims 1-7, 14-15, and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ober et al. (U.S. Patent Number 6,708,273) hereinafter referred to as Ober, in view of Childs et al. (U.S. Patent 5,623,545) hereinafter referred to as Childs, Schneier (Applied Cryptography) hereinafter referred to as Schneier, Turner et al. (U.S. Patent Number 4,896,296) hereinafter referred to as Turner, and further in view of Batcher (U.S. Patent Number 4,314,349) hereinafter referred to as Batcher.

14. Regarding claim 1, Ober disclosed an integrated circuit for performing security functions including the SHA-1 and MD5 hash algorithms (See Ober Figure 1 Element 30). However, Ober failed to disclose an embodiment for the implementation of the two hash functions.

Childs teaches a hardware implementation of the SHA-1 algorithm. The implementation includes five registers for storing chaining variables as called for by the SHA-1 algorithm (See Childs Fig. 5 elements 508-512). Childs teaches a function circuit receiving chaining variables B, C, and D (See Childs

Fig. 5 Element 516). Childs also teaches a summing circuit (Elements 520-523) receiving the output of the function circuit (f_e) and the fourth chaining variable (E) and the output coupled to the register file through a multiplexer (Element 507) (See Childs Fig. 5).

Schneier teaches that the MD5 algorithm has the same elements shown above for the SHA-1 algorithm, except that there is not a fifth chaining variable 'E' as in SHA-1 (See Schneier Page 438 Fig. 18.6).

Turner teaches that by using a multiplexer, with one input set to zero, the other inputs can be selectively excluded from the input to another function (See Turner Col. 7 Paragraph 4).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Childs and Schneier in the invention of Ober in order to carry out the hashing functions. This would have been obvious because one of ordinary skill in the art would have been motivated to provide the full functionality of the IPSec protocol when implementing this protocol.

It also would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Turner in the combination of Ober, Childs, and Schneier in order to selectively exclude the fifth chaining variable (E) from the inputs to the summing circuit in such a manner that when SHA-1 is being performed, the fifth chaining variable is passed through the multiplexer, and when MD5 is being performed, the zero is passed through the multiplexer. This would have been obvious because one of ordinary skill in the art would have been motivated to utilize the multiplexer in order to minimize the elements in the circuit of Ober, as evidenced by Batcher (See Batcher Col. 6 Paragraph 3).

15. Claim 2 recites a barrel shifter, coupled to an adder, coupled to a multiplexer, all coupled to the output of the summing circuit. MD5 requires a shifter and adder coupled to the output of the summer, as can be seen in the two rightmost elements of figure 18.6 (See Schneier Page 438). Claim 2 further recites the other input of the multiplexer being coupled to the output of the summing circuit. SHA-1 does not require the shifter or the adder at the output of the summing circuit.

It would have been obvious to employ the teachings of Batcher in order to multiplex the elements of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

16. Claim 3 recites a third multiplexer coupled to the output of the second multiplexer and also coupled to the register file to receive a fifth chaining variable (A). Childs disclosed that chaining variable B had input from chaining variable A during SHA-1 (See Childs Fig. 5 Elements 508 and 509). Schneier disclosed that chaining variable B had input from the result of the adder (See Schneier Page 436 Paragraph 9 – Page 437 Paragraph 1).

Claim 3 further recites a fourth multiplexer coupled to the output of the second multiplexer and to the register file for receiving the third chaining variable (D). Childs disclosed that chaining variable A had input from the summing circuit during SHA-1 (See Childs Fig. 5 Elements 507, 508, and 523). Schneier disclosed that chaining variable A was coupled to the chaining variable D (See Schneier Page 437 Lines 18-21).

It would have been obvious to employ the teachings of Batcher in order to multiplex the elements of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

17. Claims 4-5 were inherent in the combination of Ober, Childs, Schneier, Batcher and Turner, in order for proper operation of the MD5 and the SHA-1 when each was selectively performed in Ober. This was inherent because the MD5 algorithm must have received the correctly multiplexed inputs for MD5 and the SHA-1 must have received the correctly multiplexed inputs for SHA-1 in order for the hashes to be calculated correctly.

18. Regarding claim 6, Childs disclosed a shift circuit and a fifth multiplexer for selectively shifting the second chaining variable (B) for input to the third chaining variable (C) (See Childs Fig. 5 Elements 509, 518, 517, and 510).

19. Regarding claim 7, Childs disclosed a shift circuit receiving chaining variable A and outputting to the summing circuit in accordance with SHA-1 (See Childs Fig. 5 Elements 508, 519, 520, and 522). Schneier disclosed chaining variable A being input to the summing circuit in accordance with MD5 (See Schneier Figure 18.6).

It would have been obvious to employ the teachings of Batcher in order to multiplex the elements of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

20. Claim 14 recites a register file for storing five chaining variables, in which the five variables are preloaded for each of two algorithms. Childs depicted a register file for storing five chaining variables (See Childs Fig. 5 Elements 508-512) and also disclosed loading the registers with preset values at the beginning of the SHA-1 algorithm (See Childs Fig. 5 Element 507 and Col. 1 Lines 25-32). It was inherent in the combination of Ober, Childs, Schneier, Batcher and Turner, that when MD5 was being performed, the initial MD5 variables were loaded into the register file (See Schneier Page 436 Lines 33-38).

Claim 14 further recites a function circuit receiving three of the chaining variables and producing a logical value dependant on the algorithm being performed. Childs disclosed a function circuit taking three chaining variables and producing a logical value for the SHA-1 algorithm (See Childs Fig. 5 Element 516). Schneier disclosed a function, for the MD5 algorithm, which took three chaining variables and produced a logical output (See Schneier Page 437 Lines 5-11). These functions are different for SHA-1 and MD5 (See Childs Col. 1 Table at Line 20 and Schneier Page 437 Lines 5-11).

Claim 14 also recites a storage element for providing a set of constants for each algorithm to a summing circuit, and the summing circuit also receiving the output of the function circuit (See rejection of claim 8 regarding the storage circuit).

21. Claim 15 recites a register array, with a plurality of registers and a decoder circuit for selecting a word from the register array for the first algorithm (See Childs Fig. 6 Elements 602, and 603 and Schneier Page 437 Line 16 – Page 440 Line 17).

22. Claim 17 recites an output of the array being supplied from a word-wise circular queue when computing a second algorithm (See Childs Fig. 6 Element 602, 603, and 604).

23. Claim 18 recites the first algorithm being MD5 and the second algorithm being SHA-1. Schneier disclosed the first algorithm being MD5 (See Schneier Page 436) and Childs disclosed the second algorithm being supplied by FIPS PUB 180-1 (See Childs Abstract), which is the SHA-1 algorithm.

24. Claims 8-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ober, Childs, Schneier, Turner, and Batcher, as applied to claim 1 above, and further in view of Niehaus et al (US Patent Number 4,399,517) hereinafter referred to as Niehaus.

25. Regarding claim 8, the combination of Ober, Childs, Schneier, Turner, and Batcher disclosed a storage circuit (See Childs Fig. 5 Element 515), a register array providing W_t (See Childs Fig. 5 Element 514), a register file for storing chaining variables A-E (See Childs Fig. 5 Elements 508-512), and a summing circuit (See Childs Fig. 5 Elements 520-523) receiving constants from the storage circuit (See Childs Fig. 5 Elements 515 and 520), one input coupled to the register array (See Childs Fig. 5 Elements 514 and 520), one input coupled to either chaining variable A or a shifted version of chaining variable A depending on the mode of operation (See rejection for claim 7 above), one input for receiving a logical function in accordance with chaining variables 1, 2, and 3 (See Childs Fig. 5 Element 516), and one input providing a fourth chaining variable or a zero depending on the mode of operation (See rejection of claim 1 above).

The combination of Ober, Childs, Schneier, Turner, and Batcher further disclosed the storage circuit storing two sets of constants, one for SHA-1 and one set for MD5. Childs disclosed storing the set K_t for SHA-1 (See Childs Fig. 5 Element 515 and Col. 8 Paragraph 3) and although Schneier did not

specifically disclose storing the constants for MD5, it was inherent that they were stored in order to have performed the 64 steps in the four rounds as required by the MD5 algorithm (See Schneier Pages 438-440 t_i).

It would have been obvious to employ the teachings of Batcher in order to multiplex the constants of the SHA-1 algorithm and the MD5 algorithm in order to minimize the elements in the Hash Block of Ober.

However, the combination of Ober, Childs, Schneier, Turner, and Batcher failed to disclose the summing circuit being an adder.

Niehaus teaches a multiple input adder, which takes up to six inputs and provides the sum of the inputs (See Niehaus Abstract), and the advantages of this adder (See Niehaus Col. 1 Lines 41-48).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Niehaus in the Hash Block of the combination of Ober, Childs, Schneier, Turner, and Batcher by providing the multiple input adder in place of the summing circuit. This would have been obvious because the ordinary person skilled in the art would have been motivated to minimize gate delay as well as the fan in of the inputs.

26. Claim 9 is rejected for the same reasons as claim 1 as applied to claim 8 above.

27. Claim 10 is rejected for the same reasons as claim 2 as applied to claim 9 above.

28. Claim 11 is rejected for the same reasons as claim 3 as applied to claim 10 above.

29. Claim 12 is rejected for the same reasons as claim 6 as applied to claim 11 above.

30. Claim 13 is rejected for the same reasons as claim 7 as applied to claim 12 above.

31. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Ober, Childs, Schneier, Turner, and Batcher as applied to claim 15 above, and further in view of Masaki (US patent Number 4,739,195).

The combination of Ober, Childs, Schneier, Turner, and Batcher disclosed the register array forming a word wise circular queue (See Childs Fig. 6 Elements 602, 603, 605, 608, and 601), an exclusive-OR receiving four data words from the register file (See Childs Fig. 6 Elements 603, 605, and 606), and a shift register coupled to the output of the exclusive-OR for providing input to the register file (See Childs Fig. 6 Elements 605, 607, 608, 601, and 602). The combination of Ober, Childs, Schneier, Turner, and Batcher disclosed the shift being a one-bit shift (See Childs Abstract). However, the combination of Ober, Childs, Schneier, Turner, and Batcher failed to disclose that the data words received by the XOR were received simultaneously.

Masaki teaches that instead of using a two input XOR to XOR four inputs, a four input XOR gate can be used to provide the output in less time (See Masaki Col. 1 Lines 9-24).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Masaki in the Hash Block of the combination of Ober, Childs, Schneier, Turner, and Batcher by using a four input XOR gate instead of the two input XOR gate of Childs in order to XOR the four data words. This would have been obvious because ordinary person skilled in the art at the time of invention would have been motivated provide the result of the XOR operation in less time.

Response to Arguments

32. Applicant's arguments filed 9/21/2004 have been fully considered but they are not persuasive.

33. Applicant traverses primarily that I. Childs does not provide any reason for combining with Ober, Schneier, Turner, or Batcher, II. The examiner used hindsight in forming the obviousness rejections applied to claims 1-7, and 14-18, III. The applicant's invention is faster than the prior art because the applicant uses a parallel adder while the adder of Childs was a serial adder, all of which have been addressed below. The applicant also made significant amendments to claims 1, 8, 15, 16, and 17, which have been addressed above.

34. Regarding the applicant's argument I., applicant traverses primarily that it would not have been obvious to the ordinary person skilled in the art at the time of invention to combine the references provided in the rejection. The examiner disagrees for the reasons expressed below, and further maintains the rejections set forth in the FAOM.

35. The examiner notes that applicant has mischaracterized the rejection made in the FAOM. Applicant seems to believe that Child is the main reference applied to claims 1 and 14, and as such there is no reason to combine the references. However, in fact, as is clearly stated in the rejection presented in the FAOM, Ober is the primary reference for this rejection.

36. Ober provides a solid base by combining the well known MD5 and the well known SHA-1 hash algorithms into one Hash Block Circuit, shown in Fig. 1 Element 30 of Ober. However, because the specification of Ober did not provide the necessary circuitry or the Hash Block, any construction of the cryptographic co-processor of Ober would have required the constructor to use known circuitry for the Hash Block, and more specifically for the Hash functions themselves. Childs provided a known implementation of the SHA-1 hash algorithm, which is shown in Fig. 5. Schneier provided a diagram of the known MD5 algorithm. The ordinary person skilled in the art at the time of invention, when looking at the MD5 circuitry and the SHA-1 circuitry side by side, would see that much of the circuitry is the same, and that the main difference is that MD5 does not have a fifth chaining variable. Simply by looking at Childs Fig. 5 and Schneier Fig. 18.6, one of ordinary skill in the art would have seen the similarities between the two circuits.

37. Turner teaches that by using a multiplexer with one input set to zero, and the other set to a variable input, the variable input can be selectively excluded from the input of another function (See Turner Col. 7 Paragraph 4). Because the main difference between MD5 and SHA-1 is that a fifth chaining is used in SHA-1 and not in MD5, the ordinary person skilled in the art would have realized that a multiplexer could be used to selectively exclude the fifth chaining variable from the SHA-1 algorithm to

get the MD5 algorithm. However, Turner did not expressly teach a benefit of selectively excluding an input to a function.

38. Batcher teaches that circuit elements can be kept to a minimum by utilizing multiplexers to select between inputs of a function (See Batcher Col. 6 Paragraph 3). The ordinary person skilled in the art would realized that by utilizing the teachings of Turner by selectively excluding the fifth chaining variable of the SHA-1 of Childs to get MD5, the circuit elements of the Hash Block of Ober could be kept to a minimum.

39. In response to applicant's argument II, that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). As evidenced by the previous paragraphs, the ordinary person skilled in the art would have found all the necessary teachings and motivation to combine the references used in the 103 rejection of claims 1 and 14 above, in the teachings of the references and from general knowledge in the art. Therefore, the combining of Ober, Childs, Schneier, Turner, and Batcher in the 103 rejections of claims 1-18 did not apply improper hindsight.

40. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the motivation to combine is taught by

Batcher, in that the elements in the circuit could be minimized. Furthermore, the motivation to combine Childs with Schneier is provided by the need for both SHA-1 and MD5 in the Hash Block of Ober.

41. Regarding claims 2-7, and 9-13, the applicant applied the same arguments as already addressed for claim 1 above and therefore the examiner has maintained the rejections set forth in the FAOM.

42. Applicant's arguments III, with respect to claim 8, have been considered but are moot in view of the new ground(s) of rejection necessitated by amendment.

Conclusion

43. Claims 1-18 have been rejected.

44. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

45. Any inquiry concerning this communication should be directed to Matthew Henning whose telephone number is (571) 272-3790. The examiner can normally be reached Monday-Friday from 9am to 4pm, EST. If attempts to reach examiner by telephone are unsuccessful, the examiner's acting supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (703) 305-3900.

Matthew Henning
Assistant Examiner
Art Unit 2131

1/10/05

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER